WHAT IS CLAIMED IS:

1. A method for detecting unauthorized access, comprising:

receiving a voice input associated with a request to access an account;

generating a request voice signature corresponding to the voice input associated with the request;

retrieving an authorized voice signature corresponding to the account;

comparing the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account; and

detecting unauthorized access in response to the comparison.

2. The method of Claim 1, further comprising:

authorizing a user for the account; and

generating the authorized voice signature corresponding to the authorized user.

3. The method of Claim 1, further comprising:

authorizing a user for the account;

receiving an authorized voice input corresponding to the authorized user; and

generating the authorized voice signature according to the authorized voice input.

4. The method of Claim 1, wherein generating the request voice signature corresponding to the voice input associated with the request comprises:

determining a request feature vector corresponding to the voice input; and

generating the request voice signature according to the request feature vector.

5. The method of Claim 1, wherein comparing the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account comprises:

establishing a request feature vector corresponding to the request voice signature, the request feature vector comprising a plurality of first values, each first value corresponding to a variable of a plurality of variables;

establishing an authorized feature vector corresponding to the authorized voice signature, the authorized feature vector comprising a plurality of second values, each second value corresponding to a variable of the plurality of variables, each second value corresponding to a first value; and

comparing each first value with the corresponding second value to compare the request voice signature with the authorized voice signature.

6. The method of Claim 1, further comprising:

accessing a fraudulent voice signature file; and

identifying a user associated with the request voice signature in accordance with the fraudulent voice signature file.

7. The method of Claim 1, further comprising:

accessing a fraudulent voice signature file;

determining if the fraudulent voice signature file comprises the request voice signature; and

adding the request voice signature to the fraudulent voice signature file if the fraudulent voice signature file does not comprise the request voice signature.

8. The method of Claim 1, further comprising denying access to the account in response to detecting the unauthorized access.

9. A system for detecting unauthorized access, comprising:

a database operable to store an authorized voice signature corresponding to an account; and

a processor coupled to the database and operable to:

receive a voice input associated with a request to access the account;

generate a request voice signature corresponding to the voice input associated with the request;

retrieve the authorized voice signature corresponding to the account;

compare the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account; and

detect unauthorized access in response to the comparison.

10. The system of Claim 9, the processor further operable to:

authorize a user for the account; and

generate the authorized voice signature corresponding to the authorized user.

11. The system of Claim 9, the processor further operable to:

authorize a user for the account;

receive an authorized voice input corresponding to the authorized user; and

generate the authorized voice signature according to the authorized voice input.

12. The system of Claim 9, the processor further operable to generate the request voice signature corresponding to the voice input associated with the request by:

determining a request feature vector corresponding to the voice input; and

generating the request voice signature according to the request feature vector.

13. The system of Claim 9, the processor further operable to compare the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account by:

establishing a request feature vector corresponding to the request voice signature, the request feature vector comprising a plurality of first values, each first value corresponding to a variable of a plurality of variables;

establishing an authorized feature vector corresponding to the authorized voice signature, the authorized feature vector comprising a plurality of second values, each second value corresponding to a variable of the plurality of variables, each second value corresponding to a first value; and

comparing each first value with the corresponding second value to compare the request voice signature with the authorized voice signature.

14. The system of Claim 9, the processor further operable to:

access a fraudulent voice signature file; and

identify a user associated with the request voice signature in accordance with the fraudulent voice signature file.

15. The system of Claim 9, the processor further operable to:

access a fraudulent voice signature file;

determine if the fraudulent voice signature file comprises the request voice signature; and

add the request voice signature to the fraudulent voice signature file if the fraudulent voice signature file does not comprise the request voice signature.

16. The system of Claim 9, the processor further operable to deny access to the account in response to detecting the unauthorized access.

17. A method for identifying a fraudulent voice signature, comprising:

accessing a fraudulent voice signature file comprising a plurality of fraudulent voice signatures;

receiving a user voice signature;

comparing the user voice signature to at least a portion of the plurality of fraudulent voice signatures;

determining whether the user voice signature matches a fraudulent voice signature; and

identifying the user voice signature as fraudulent if the user voice signature matches a fraudulent voice signature.

18. The method of Claim 17, wherein comparing the user voice signature to at least the portion of the plurality of fraudulent voice signatures comprises:

establishing a user feature vector corresponding to the user voice signature, the user feature vector comprising a plurality of first values, each first value corresponding to a variable of a plurality of variables;

establishing a fraudulent feature vector corresponding to the fraudulent voice signature, the fraudulent feature vector comprising a plurality of second values, each second value corresponding to a variable of the plurality of variables, each second value corresponding to a first value; and

comparing each first value with the corresponding second value.

19. A system for identifying a fraudulent voice signature, comprising:

a database operable to store a fraudulent voice signature file comprising a plurality of fraudulent voice signatures; and

a processor coupled to the database and operable to:

receive a user voice signature;

compare the user voice signature to at least a portion of the plurality of fraudulent voice signatures;

determine whether the user voice signature matches a fraudulent voice signature; and

identify the user voice signature as fraudulent if the user voice signature matches a fraudulent voice signature.

20. The system of Claim 19, the processor operable to compare the user voice signature to at least the portion of the plurality of fraudulent voice signatures by:

establishing a user feature vector corresponding to the user voice signature, the user feature vector comprising a plurality of first values, each first value corresponding to a variable of a plurality of variables;

establishing a fraudulent feature vector corresponding to the fraudulent voice signature, the fraudulent feature vector comprising a plurality of second values, each second value corresponding to a variable of the plurality of variables, each second value corresponding to a first value; and

comparing each first value with the corresponding second value.

21. A system for detecting unauthorized access, comprising:

means for receiving a voice input associated with a request to access an account;

means for generating a request voice signature corresponding to the voice input associated with the request;

means for retrieving an authorized voice signature corresponding to the account;

means for comparing the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account; and

means for detecting unauthorized access in response to the comparison.

22. A method for detecting unauthorized access, comprising:

authorizing a user for an account;

receiving an authorized voice input corresponding to the authorized user;

generating an authorized voice signature corresponding to the account according to the authorized voice input;

receiving a voice input associated with a request to access the account;

generating a request voice signature corresponding to the voice input associated with the request by:

determining a request feature vector corresponding to the voice input; and

generating the request voice signature according to the request feature vector;

retrieving the authorized voice signature corresponding to the account;

comparing the request voice signature corresponding to the voice input with the authorized voice signature corresponding to the account by:

establishing a request feature vector corresponding to the request voice signature, the request feature vector comprising a plurality of first values, each first value corresponding to a variable of a plurality of variables;

establishing an authorized feature vector corresponding to the authorized voice signature, the authorized feature vector comprising a plurality of second values, each second value corresponding to a variable of the plurality of variables, each second value corresponding to a first value; and

comparing each first value with the corresponding second value to compare the request voice signature with the authorized voice signature;

detecting unauthorized access in response to the comparison;

denying access to the account in response to detecting the unauthorized access;

accessing a fraudulent voice signature file comprising a plurality of fraudulent voice signatures;

determining if the fraudulent voice signature file comprises the request voice signature;

adding the request voice signature to the fraudulent voice signature file if the fraudulent voice signature file does not comprise the request voice signature;

identifying a user associated with the request voice signature in accordance with the fraudulent voice signature file;

receiving a user voice signature;

comparing the user voice signature to at least a portion of the plurality of fraudulent voice signatures;

determining whether the user voice signature matches a fraudulent voice signature; and

identifying the user voice signature as fraudulent if the user voice signature matches a fraudulent voice signature.